

REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 4-20 and 30-35 are currently pending in this application. Claim 36 has been newly added by this reply. Claims 30, 31, 34, and 35 are independent. The remaining claims depend, directly or indirectly, from claims 30 and 31.

New Claim 36

Claim 36 has been newly added by this reply. No new subject matter is added by way of the newly added claim. Claim 36 recites a receiver/decoder operatively connected to a recording means and configured to receive encrypted transmitted digital data, where the recording means records the encrypted transmitted digital data and an encrypted recording encryption key to a recording support medium. Support for the newly added claim may be found in the original claims and the Specification as filed.

Rejections under 35 U.S.C. § 102

Claims 4-8, 14-16, 30-32, 34, and 35 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,991,400 ("Kamperman"). This rejection is respectfully traversed.

Turning to the rejection of the claims, for anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. The Applicant respectfully asserts that Kamperman does not teach or suggest encrypting transmitted digital data.

As described previously, the claimed invention recites that *transmitted* digital information is encrypted with a recording encryption key, and the recording encryption key is then encrypted using a recording transport key. Further, the recording encryption key and/or the recording transport key are stored on a recording medium along with the encrypted transmitted digital information.

In contrast to the claimed invention, Kamperman discloses that EMMs are decrypted to obtain an authorization key (AK). The AK is then used to decrypt ECMs to obtain control words (CWs) (*see* Kamperman, col. 5, ll. 34-40). Kamperman then discloses that a pay-TV program is received and stored, together with the accompanying ECMs that comprise the necessary CWs (*see* Kamperman, col. 5, ll. 53-58). Finally, Kamperman discloses that the AK is encrypted to provide an encrypted AK that is recorded together with the pay-TV program (*see* Kamperman, col. 6, ll. 50-57). Thus, it is clear that in Kamperman, the pay-TV program is stored as received, and an encrypted AK is added to the recording medium. Further, in Kamperman, the AK is used to *decrypt* ECMs rather than to *encrypt* any type of data.

The Examiner asserts that col. 4, ll. 49-54 of Kamperman disclose encrypting transmitted digital information. The Applicant respectfully disagrees. The MMG that encrypts the AK in Kamperman is located at the *transmission end* (*see* Kamperman, Figure 1). Thus, it is not possible for the MMG to encrypt *transmitted* data; the MMG can only encrypt data *to be* transmitted.

Further, even assuming *arguendo* that Kamperman does disclose encrypting transmitted digital data, Kamperman still fails to disclose or suggest encrypting the encryption key that is used to encrypt the CWs. That is, Kamperman discloses that CWs are

encrypted by a control word encrypter (CWE). However, the key used to encrypt the CWs is not itself encrypted, as required by the claims of the present invention. In the present invention, the transmitted digital data, including a CW is encrypted using a recording encryption key. The recording encryption key is then encrypted using a recording transport key. However, Kamperman fails to disclose this additional step. Rather, Kamperman goes on to disclose that the AK is encrypted by the MMG. However, because the AK is *not* the key used to encrypt the CWs, Kamperman fails to disclose the independent claims as recited.

In view of the above, it is clear that Kamperman fails to disclose or suggest all the limitations of independent claims 30, 31, 34, and 35. Further, dependent claims 4-8, 14-16, and 32 are patentable over Kamperman for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 9-13 and 33 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Kamperman in view of U.S. Patent No. 5,621,793 ("Bednarek"). This rejection is respectfully traversed.

As described above, Kamperman fails to disclose all the limitations of independent claims 30 and 31. Further, Bednarek fails to supply that which Kamperman lacks. Specifically, Bednarek discloses a set-top box with a global positioning system (GPS) receiver. The GPS receiver checks to see if the set-top box is at an authorized location and allows descrambling of video signals only if the location is authorized (*see* Bednarek, Abstract). Bednarek fails to disclose or suggest encrypting transmitted digital information, which includes a CW. Further, Bednarek is completely silent with respect to encrypting the encryption key used to encrypt the transmitted digital information.

In view of the above, it is clear that independent claims 30 and 31 are patentable over Kamperman and Bednarek, whether considered separately or in combination. Dependent claims 9-13 and 33 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 17-20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Kamperman in view of European Patent No. 714204 ("Park"). This rejection is respectfully traversed.

As described above, Kamperman fails to disclose all the limitations of independent claim 30. Further, Park fails to supply that which Kamperman lacks. Particularly, Park relates to a method for preventing an illegal user from viewing the digital video system and copying from the digital video system. Park discloses setting a descrambling method that decrypts split keystreams using a smartcard (*see* Park, Abstract). However, Park fails to disclose or suggest encrypting transmitted digital information, which includes a CW. Further, Park is completely silent with respect to encrypting the encryption key used to encrypt the transmitted digital information and storing the encrypted transmitted digital information along with the recording encryption key and/or the recording transport key on a recording medium.

In view of the above, it is clear that independent claim 30 is patentable over Kamperman and Park, whether considered separately or in combination. Dependent claims 17-20 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

New Independent Claim 36

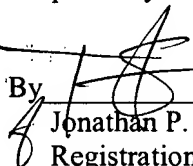
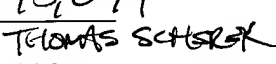
Newly added independent claim 36 recites similar subject matter as independent claims 30, 31, 34, and 35. Particularly, new independent claim 36 recited encrypted transmitted digital data and a recording encryption key that is used to encrypt the transmitted digital data, where the recording encryption key is further encrypted using a recording transport key. Thus, new independent claim 36 is patentable over Kamperman for at least the same reasons described above. Accordingly, favorable consideration of new independent claim 36 is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 11345/023001).

Dated: March 2, 2006

Respectfully submitted,

By  #45,079
Jonathan P. Osha 
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

137894_1.DOC